1. a) What is a Carmichael number? SOLUTION: A Carmichael number is a nonprime integer $n > 1$ such that $a^n \equiv a \mod n$ for all $a \in \mathbb{Z}$.

b) Prove or disprove that $n = 7 \cdot 13 \cdot 19$ is Carmichael. SOLUTION: The test for being Carmichael is that $n$ is square-free (i.e., $n = p_1 \ldots p_k$ where $p_1, \ldots, p_k$ are distinct primes), nonprime, and for all primes $p$ dividing $n$, $n \equiv 1 \mod p - 1$.

Clearly $n = 7 \cdot 13 \cdot 19$ is nonprime and square-free. For $p = 7$, note that 7, 13 and 19 are all 1 mod 6, hence so is $n$. For $p = 13$, $n \equiv 7 \cdot 1 \cdot 7 \equiv 1 \mod 12$. For $p = 19$, $n \equiv 7 \cdot 13 \cdot 1 \equiv 91 \equiv 1 \mod 18$,

and the result follows.

2. True or False. If false, give a counterexample.

a) 4 is Carmichael. SOLUTION: 4 is not square-free, so it fails the test for being Carmichael, but that is not the same as producing a counterexample. For a counterexample, note that $2^4 \equiv 0 \mod 4$ but $2 \neq 0 \mod 4$.

b) $\mathbb{Z}_{p^r}^\times$ is cyclic for all primes $p$ and all $r > 0$. SOLUTION: This is false for $p = 2$ and $r \geq 3$, so a counterexample is given by $\mathbb{Z}_8^\times$, where every nonidentity unit has order 2, so there is no element of order 4.

3. What is the order of $\overline{19}$ in $\mathbb{Z}_n^\times$ for the following choices of $n$:

a) $2^9$. SOLUTION: 19 $\equiv -1 \mod 4$, so 19 has order 2 mod 4, giving $|19| = 2|19^2|$ in $\mathbb{Z}_{2^5}^\times$. Now, $19^2 = 361 = 1 + 2^3 \cdot 3^2 \cdot 5$,

so $|19^2| = 2^9 - 3 = 2^6$, hence $|19| = 2 \cdot 2^6 = 2^7$.

b) $3^8$. SOLUTION: 19 $\equiv 1 \mod 3$: 19 = 1 + $3^2 \cdot 2$, so $|19| = 3^8 - 2 = 3^6$ in $\mathbb{Z}_{3^8}^\times$.

c) $7^6$. SOLUTION: 19 $\equiv 5 \mod 7$, and 5 has order 6 in $\mathbb{Z}_7^\times$, so $|19| = 6|19^6|$ in $\mathbb{Z}_{7^6}^\times$. Now, $19^6 = 47045881 = 1 + 7^3 \cdot 137160$. 

Exam 2 Solutions

Where \((137160, 7) = 1\), so \(|19^6| = 7^{6-3} = 7^3\) in \(\mathbb{Z}_7^\times\). So \(|19| = 6|19^6| = 6 \cdot 7^3\) in \(\mathbb{Z}_7^\times\).

d) \(2^9 3^8 7^6\). Solution: We have found the order of 19 modulo each of the prime powers dividing \(n\), so we just take the least common multiple of those numbers:

\[|19| = [2^7, 3^6, 6 \cdot 7^3] = 2^7 3^6 7^3\] in \(\mathbb{Z}_n^\times\).

4. a) What is the smallest nonnegative integer congruent to \(8^{3982702498462}\) mod 13? Solution: write \(n = 3982702498462\) here and in the next part. We first find the order of 8 in \(\mathbb{Z}_{13}^\times\). We have \(8^2 \equiv 12 \equiv -1\) mod 13, so \(8^4 \equiv 1\) mod 13, hence the order divides 4. Since we’ve tested all the divisors of 4, the order is exactly 4. Now, since \(4|100\), \(n \equiv 62 \equiv 2\) mod 4. So \(n = 4q + 2\) for some \(q\). Now,

\[8^n = 8^{4q+2} = (8^4)^q \cdot 8^2 \equiv 1^q \cdot 8^2 \equiv -1 \equiv 12\] mod 13,

so the answer is 12.

b) What is the order of \(8^{3982702498462}\) in \(\mathbb{Z}_{13}^\times\)? Solution:

\[|8^n| = \frac{|8|}{(n, |8|)} = \frac{4}{(n, 4)} = \frac{4}{2} = 2.\]

5. Find the smallest nonnegative solution for the following congruences.

\[x \equiv 1 \mod 90\]
\[x \equiv 91 \mod 250\]
\[x \equiv 41 \mod 100\]

Solution: We first solve the first two congruences, getting

\[1 + 90k = 91 + 250\ell\]
\[250(-\ell) + 90k = 90 = 9 \cdot 10,\]

where we note that \((250, 90) = 10\). Solving Bezout’s identity for 250 and 90, we get

\[10 = 4 \cdot 250 + (-11) \cdot 90\]
\[90 = 9 \cdot 10 = 36 \cdot 250 + (-99) \cdot 90,\]
so we can take \( \ell = -36 \) and \( k = -99 \). This gives
\[
x \equiv 91 + (-36) \cdot 250 \mod [250,90] = \frac{90 \cdot 250}{10} = 9 \cdot 250
\]
\[
\equiv 91 + 0 \cdot 250 \mod 9 \cdot 250,
\]
as \(-36 \equiv 0 \mod 9\)
\[
\equiv 91 \mod 2250.
\]
(Note: we could simply have solved \( 250(-\ell) + 90k = 90 \) by taking \( \ell = 0 \) and \( k = 1 \) and gotten the same result, saving a lot of work. I did not see that right off, and I’m sure many of you didn’t either.)

We now solve
\[
x \equiv 91 \mod 2250
\]
\[
x \equiv 41 \mod 100,
\]
so
\[
41 + 100k = 91 + 2250\ell,
\]
\[
2250(-\ell) + 100k = 50.
\]
Solving Bezout’s identity for 2250 and 100 gives
\[
50 = 2250 + (-22) \cdot 100,
\]
giving \( \ell = -1 \) and \( k = -22 \). So
\[
x \equiv 41 + (-22) \cdot 100 \mod [2250,100] = \frac{2250 \cdot 100}{50} = 45 \cdot 100
\]
\[
\equiv 41 + 23 \cdot 100
\]
as \(-22 \equiv 23 \mod 45\)
\[
\equiv 2341 \mod 4500.
\]

6. Find all solutions of \( x^2 \equiv 1 \) in

a) \( \mathbb{Z}_{128} \). Solution: \( 128 = 2^7 \) so the solutions are \( \overline{1}, \overline{2^6 - 1}, \overline{2^6 + 1} \)
and \( \overline{-1} \), or \( \pm 1 \), \( 63 \) and \( 65 \).

b) \( \mathbb{Z}_{10000} \). Solution: \( 10000 = 2^4 \cdot 5^4 \). We have
\[
x^2 \equiv 1 \mod 10000 \iff x^2 \equiv 1 \mod 16 \iff x \equiv 1, 7, 9, -1 \mod 16
\]
\[
x^2 \equiv 1 \mod 625 \iff x \equiv \pm 1 \mod 625.
\]
We solve this via the Chinese remainder theorem. Bezout’s identity for 625 and 16 gives
\[ 1 = 625 - 39 \cdot 16 \]
\[ = 625 - 624. \]
Thus,
\[ 625 \equiv 1 \mod 16 \quad \text{and} \quad 625 \equiv 0 \mod 625 \]
\[ -624 \equiv 0 \mod 625 \quad \text{and} \quad -624 \equiv 1 \mod 625. \]

**Case 1:**
\[ x \equiv 1 \mod 16, \ x \equiv 1 \mod 625. \ x \equiv 1 \mod 10000. \]

**Case 2:**
\[ x \equiv -1 \mod 16, \ x \equiv 1 \mod 625. \]
\[ x \equiv -1 \cdot 625 + 1 \cdot (-624) \equiv -1249 \equiv 8751 \mod 10000. \]

**Case 3:**
\[ x \equiv 7 \mod 16, \ x \equiv 1 \mod 625. \]
\[ x \equiv 7 \cdot 625 + 1 \cdot (-624) \equiv 3751 \mod 10000. \]

**Case 4:**
\[ x \equiv 9 \mod 16, \ x \equiv 1 \mod 625. \]
\[ x \equiv 9 \cdot 625 + 1 \cdot (-624) \equiv 5001 \mod 10000. \]

**Case 5:**
\[ x \equiv 1 \mod 16, \ x \equiv -1 \mod 625. \]
\[ x \equiv -8751 \equiv 1249 \mod 10000. \]

**Case 6:**
\[ x \equiv -1 \mod 16, \ x \equiv -1 \mod 625. \ x \equiv -1 \mod 10000. \]

**Case 7:**
\[ x \equiv 7 \mod 16, \ x \equiv -1 \mod 625. \]
\[ x \equiv -5001 \equiv 4999 \mod 10000. \]

**Case 8:**
\[ x \equiv 9 \mod 16, \ x \equiv -1 \mod 625. \]
\[ x \equiv -3751 \equiv 6249 \mod 10000. \]

7. (Extra credit) Find a generator for \( \mathbb{Z}_{11^8}^\times \). **Solution:** We first find a generator of \( \mathbb{Z}_{11}^\times \). Note the order of any element of \( \mathbb{Z}_{11}^\times \) divides \( 10 = \phi(11) \), so the possible orders are 1, 2, 5, 10. Note that since neither \( 2^2 = 4 \) nor \( 2^5 = 32 \) is congruent to 1 mod 11, 2 generates \( \mathbb{Z}_{11}^\times \).

In particular, in \( \mathbb{Z}_{11^8}^\times \), \( |2| = 10 |2^{10}| \). Now, \( 2^{10} = 1024 = 1 + 11 \cdot 3 \cdot 31 \), so \( 2^{10} \) has order \( 11^8 - 1 = 11^7 \) in \( \mathbb{Z}_{11^8}^\times \). Thus \( |2| = 10 \cdot 11^7 = \phi(11^8) \), so 2 is the desired generator.